新技術説明会
New Technology Presentation Meetings!

2021年度 新技術説明会

プライバシー保護とデータ連携が両立可能な秘密計算基盤の構築

2021年10月 7日

東京理科大学　工学部　電気工学科　教授

岩村恵市

目次

Society5.0（超スマート社会）

- 我が国が目指すべき未来社会の姿
  - 内閣府の科学技術政策：第5期科学技術基本計画

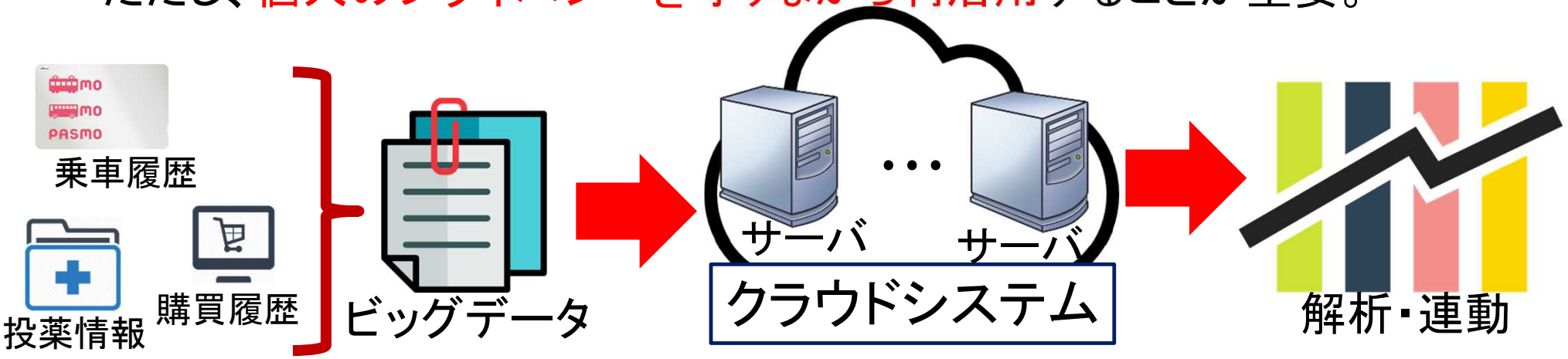
  - サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会

  - 狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）

  - キーワード：IoT、AI、ロボット　を連携⇒データ連携

研究背景

- Society5.0（超スマート社会）を実現するためには、IoTなどから得られる膨大なビッグデータを解析・連動させる技術が必要。
- ただし、個人のプライバシーを守りながら利活用することが重要。



超スマート社会に必須のデータ連携において、個人情報を漏洩させずに利活用できる仕組みを構築することが重要

研究背景

データを秘匿しながら、データ連携を含むビッグデータの利活用を安全に実現できる技術

↓

秘密計算

※入力情報を秘匿したまま、種々の計算を行うことができる

種々の処理：秘匿四則計算、秘匿データ検索（完全一致、秘匿部分一致）、等

秘密計算

・秘密計算の仕組みの代表的なものは2つある：

完全準同型暗号ベース

鍵を用いて暗号化することで秘匿性を担保

↓

公開鍵暗号を基本とし、処理が複雑なため、計算に大きなコストが必要

↓

高性能な計算機等を整備した計算環境が必要

秘密分散ベース

データを分割し物理的に計算空間を分けるというアーキテクチャで情報の秘匿性を担保

↓

計算速度は完全準同型暗号より数千倍速いが、サーバ間の高速な通信網が必要

↓

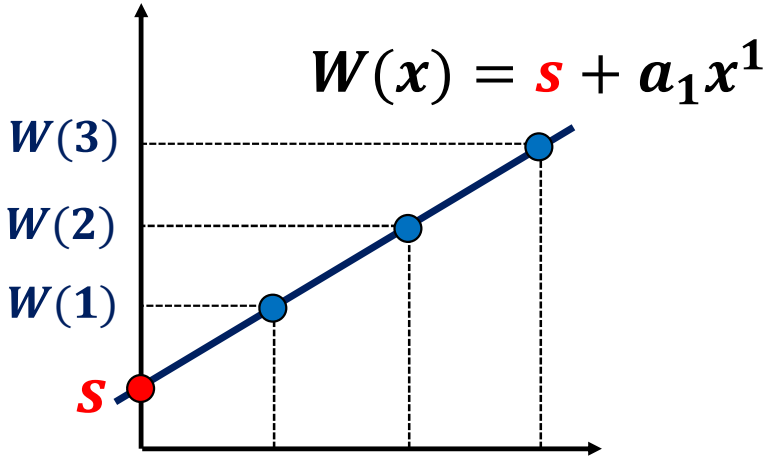
本研究は秘密分散ベースを採用するが、従来の問題点を解決した秘密計算を実現

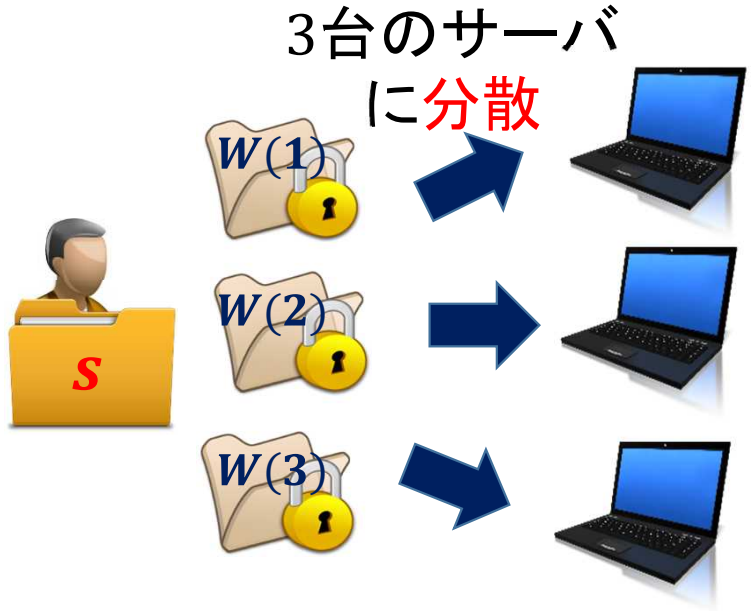
秘密分散法～(k, n)Shamir法（分散）

1. 係数a_1~a_{k-1}をランダムに定め、分散式を決定する。

$$W(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$$

例えば：$k = 2, n = 3$の場合





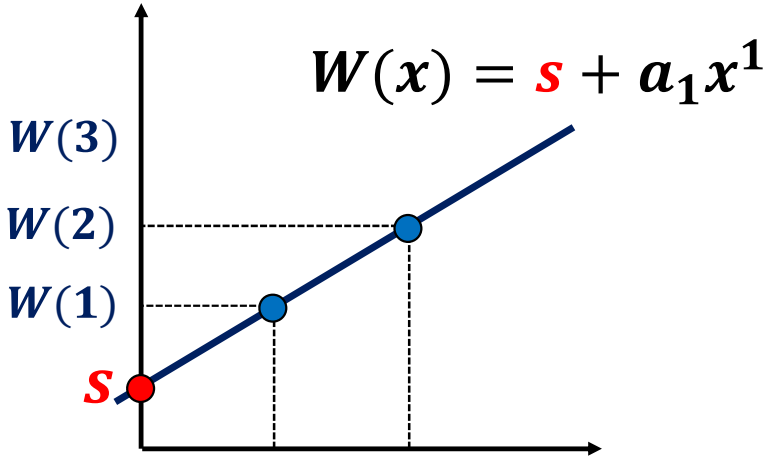
[1] A. Shamir, “How to Share a Secret”, Communications of the ACM, 22, (11), pp. 612-613, (1979)

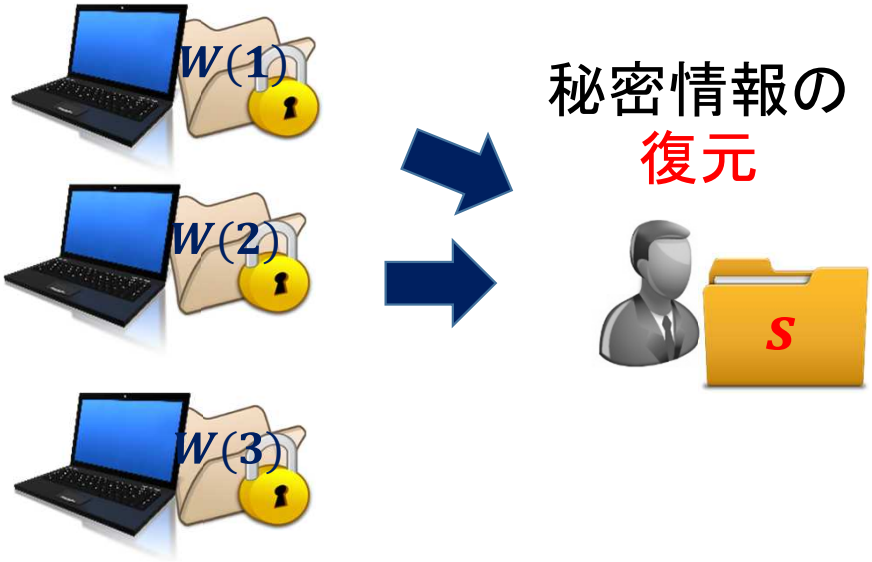
秘密分散法～(k, n)Shamir法（復元）

1. k個の分散情報Wからsとa_1~a_{k-1}を未知数として連立方程式を解く。

$$W(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$$

例えば：$k = 2, n = 3$の場合





[1] A. Shamir, “How to Share a Secret”, Communications of the ACM, 22, (11), pp. 612-613, (1979)

秘密分散を用いた秘密計算

従来技術の問題点：

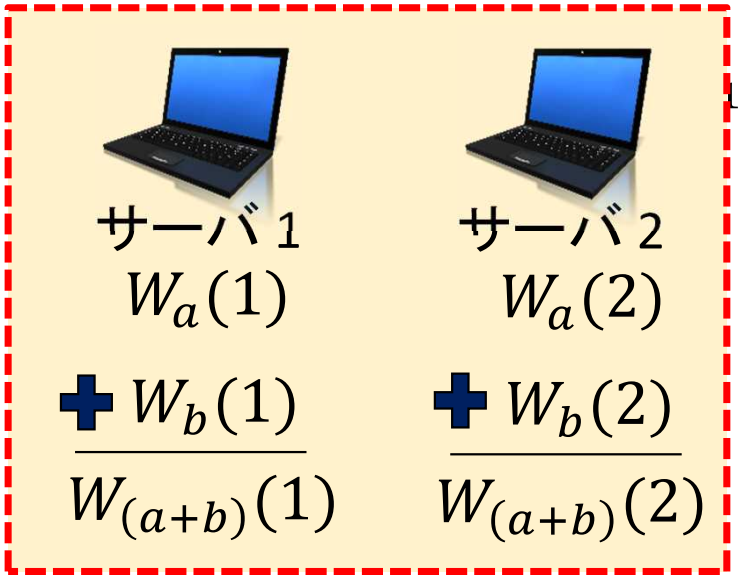
・乗算の場合、多項式の次数変化により、$n \geq 2k-1$という制限が存在する

・例えば、$k=2$の場合。

加算処理

$$W_{ai} = \boldsymbol{a} + a_1 x_i{}^1$$
$$\boldsymbol{+}\ W_{bi} = \boldsymbol{b} + b_1 x_i{}^1 \quad \} \text{1次式}$$

$$W_{(ab)i} = \boldsymbol{a+b} + (a_1 + b_1) x_i{}^{\boldsymbol{1}} \quad \} \text{1次式}$$



秘密分散を用いた秘密計算

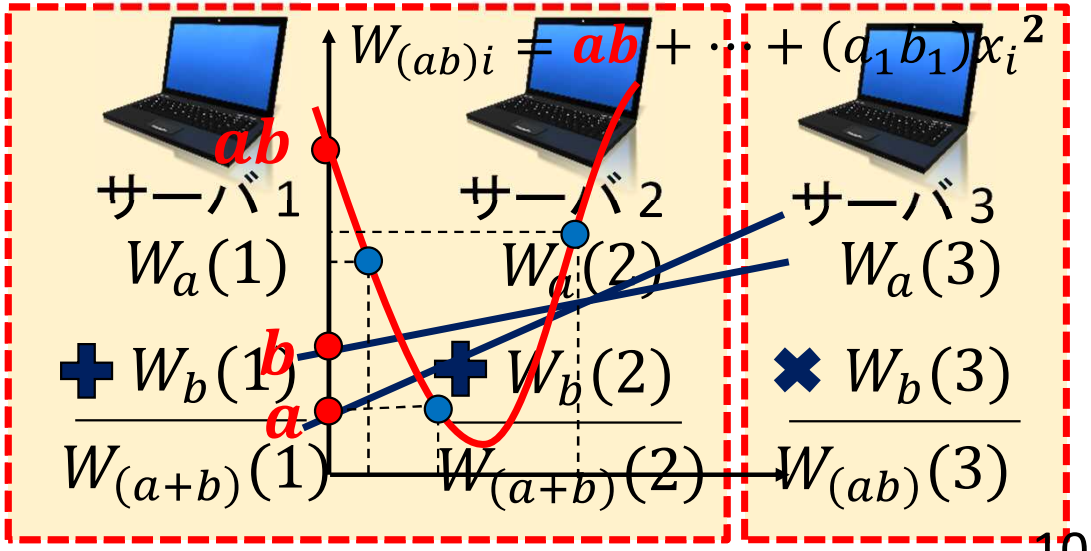
従来技術の問題点：

- 乗算の場合、多項式の次数変化により、$n \geq 2k-1$という制限が存在する
- 例えば、$k=2$の場合。
- 3台のサーバのうち、2台が攻撃されれば、情報が漏洩する

乗算処理

$$W_{ai} = \boldsymbol{a} + a_1 {x_i}^1$$
$$\times\ W_{bi} = \boldsymbol{b} + b_1 {x_i}^1 \quad \Big\} \text{1次式}$$

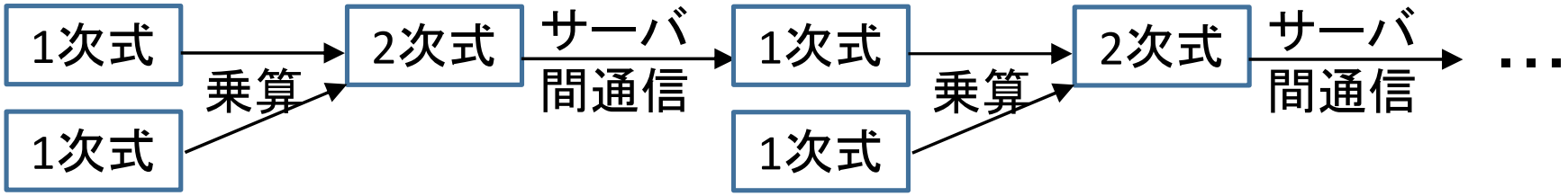
$$W_{(ab)i} = \boldsymbol{ab} + \cdots + (a_1 b_1) {x_i}^2 \quad \Big\} \text{2次式}$$



秘密分散を用いた秘密計算

従来技術の問題点2:

- 乗算による次数増を元に戻すために乗算の度にサーバ間の通信が必要
- 処理時間の短縮にはサーバ間の高速な通信網が必須
- 例えば、$k = 2$の場合。



（秒）	TUS4方式	SPDZ	Arakiらの方式
計算時間	3.30E-05	4.45E-05	3.12E-05
通信確立	0	2.06E-03	1.99E-03
通信時間	0	1.71E-03	1.36E-03
合計	3.30E-05	3.82E-03	3.37E-03

TUS方式（新技術の特徴）

- 秘密分散を用いて、n<2k-1における秘密計算を実現（最小n=1）
- 秘密情報は乱数で秘匿（暗号と秘密分散の組み合わせ）
- 事前処理により、秘密計算から通信を排除して高速化可能
- 特徴別にTUS4方式～TUS7方式が存在（TUS1～TUS3方式は旧型）
- 問題点：情報理論的に安全な乱数（物理乱数）の分散値が事前に必要（量子コンピュータなどが発達しても安全）

TUS方式の問題点の解決

- TUS方式の問題点：攻撃者が知らない物理乱数の分散値が事前に必要

解決法

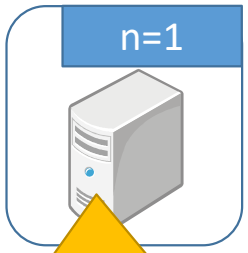
- 第三者機関（TTP：Trusted Third Party）を設置して、物理乱数の分散値を生成・配布し、利益を得られるようにする。
- 秘密計算自体は秘密計算を希望する参加者に任せる。
- （従来のビジネスモデルは秘密計算を行うことにより利益を得る）

利点

- ⇒TTPは秘密計算に関らないため、秘密情報が漏洩しても責任回避可能
- ⇒計算環境（計算機や通信網）に拘らず秘密計算によるデータ連携等が可能

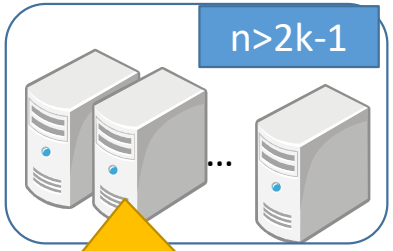
提案するビジネスモデル（従来技術との比較）

従来のビジネスモデルⅠ



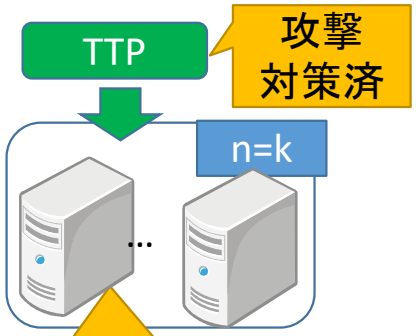
準同型暗号を用いる場合：
欠点：①処理が低速
（要高性能サーバ）
②計算量的安全性
③ユーザのみ不可
（データ委託が必要）
利点：①サーバ1台で可
②鍵が安全なら情報漏洩無し

従来のビジネスモデルⅡ



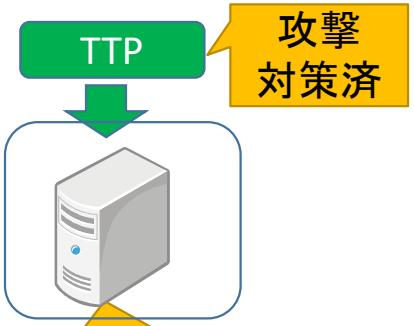
秘密分散を用いる場合：
欠点：①同一サーバ管理者には秘密情報漏洩
②ユーザのみ不可
（データ委託が必要）
利点：①処理が高速
（要高速通信網）
②情報理論的安全性

提案するビジネスモデルⅠ



K人のユーザが秘匿計算：
利点：①ユーザのみで可
（データ委託不要）
②自データの安全管理で情報漏洩無し
③処理が高速
（高速通信網不要）
④情報理論的安全性
⑤検証機能可

提案するビジネスモデルⅡ



1台のサーバで秘匿計算：
利点：①サーバ1台で可
②鍵が安全なら情報漏洩無し
③処理が高速
（高速通信網不要）
④情報理論的安全性
⑤検証機能可

秘密計算基盤の効果（想定される用途）

・どこでも誰でも秘匿計算によるデータ連携が可能

代表的応用例

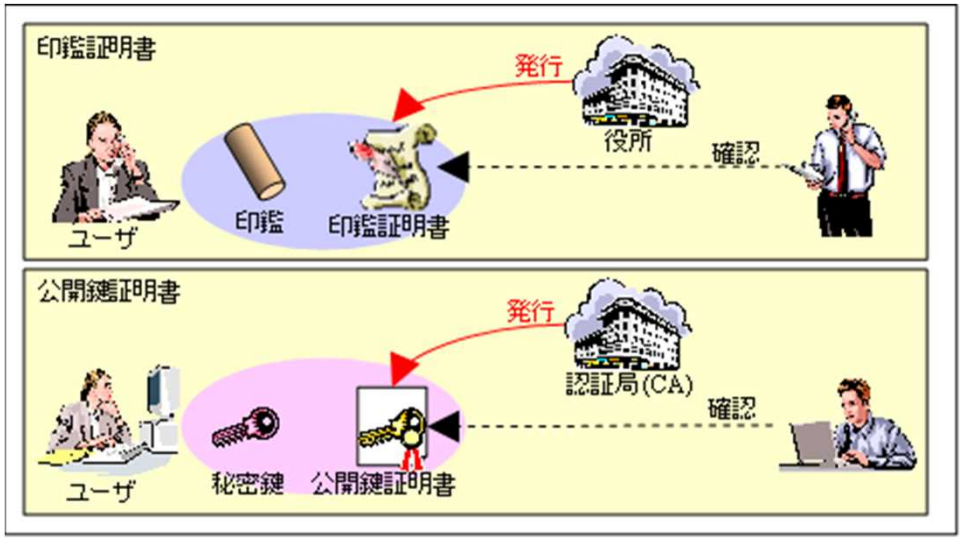
・高速な秘密検索によるリアルタイムデータ連携

・異なる業種・組織間のデータを秘匿したままでのビッグデータ解析

・AIとの組み合わせで種々の秘密解析

他のTTPビジネスとの比較

- PKI（Public Key Infrastructure）＝公開鍵基盤
  - 認証局（CA：Certification Authority）による「公開鍵証明書」発行の仕組
  - CAはTTPに相当し、公開鍵証明書の発行時、及び管理により利益を得る



- 秘密計算基盤＝SCI（Secret Computation Infrastructure）
- TTPによる秘密計算に必要な乱数を発行する仕組
- 秘密計算が行われる度に利益が得られる。

http://www.ipa.go.jp/security/pki/013.html参照

実用化に向けた課題と企業への期待

- 物理乱数を生成するTTPの構築
  - 物理雑音（熱雑音、原子核崩壊、等）から物理乱数を生成する技術との融合
- 具体的応用の実用化
  - 具体的応用をお持ちの企業と協力してその実用化
- ベンチャー起業
  - Society5.0を目指す企業とのベンチャー起業

本技術に関する知的財産権

- 特許１：（TUS方式基本特許）
  入力者装置、演算支援装置、装置、秘匿演算装置、及びプログラム
  特願2018- 28308、審査中、出願人：岩村恵市、H30.2.20、共願後単願

- 特許２：（検証機能付きTUS方式）
  分散装置、秘匿演算装置、検証復元装置、分散システム、秘匿演算検証復元システム、及びプログ ラム、特願 2018-185931、審査請求予定、出願人：東京理科大学、H30.9.28、単願

- 特許３：（TTPの構成）
  第三者装置、秘匿計算システム、及びプログラム、特願2021-108577
  2021.6.30出願、出願人：東京理科大学、R3.6.30、単願

産学連携の経歴

・データセキュリティ関連企業との共同研究実績あり
（秘密分散、ブロックチェーンなど）

まとめ

- 秘密計算基盤（SCI）によって、どこでもだれでも秘密計算によるデータ連携が可能になる
- Society5.0（超スマート社会）が進めば、プライバシーを保護した（秘密計算による）データ連携が必須となり、TTPのビジネスも広がる
- 社会が目指すSociety5.0の実現に貢献し、新たなビジネスを創出

お問い合わせ先

東京理科大学
研究戦略・産学連携センター　辻本　明

ＴＥＬ　03-5228-7431
ＦＡＸ　03-5228-7442
e-mail　tsujimoto_akira@admin.tus.ac.jp